Copy of #12

Not Conve

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant and Inventor	Ho Keung, TSE.
Title	
Filing Date	07/09/98
Application Number	09/112,276
Group Art Unit	2132
Examiner	Gilberto Barron Jr.
Postal Address	P.O. Box 54670, North Point Post Office, Hong Kong.
H.K. Tel & FAX	(852) 8105, 1090 (852) 8105, 1091
Email	t9224@netscape.net

By Airmail ~~***& Fax***~~

Hon. Commissioner of Patents and Trademarks, Washington, D.C. 20231.

Sir,

Submission of Clean Claims

The clean claims submitted herewith includes all the changes in claims requested by Amendment Proposals dated 7 May, 2001 and dated 17, June 2001.

Respectfully submitted,

Ho Keung, Tse.

1.(Third time Amended) A method for protecting software from unauthorised use , comprising the steps of :

determining if identity means/information, is existing in a processing device ;

using a favourable result of said determination as a pre-condition for said processing device providing user access to said software desired to be protected ;

wherein said identity means/information being used by a control means of said processing device for

enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) .

2. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein further comprising the steps of :

authenticating said identity means/information ;

said identity means/information will be determined as existing, if the result of said authentication is favourable and as not existing if otherwise .

3. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being a first software used on said processing device for determining third information related to hardware and/or software of said processing device ;
wherein further comprising second software for , when being executed, authenticating the computer on which said second software runs as being said processing device, basing on at least a part of said third information;
and access to a third software will be provided if said authentication result is favourable ;
wherein said third software being distributed through a communication network to said rightful user.

4. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful user(s).

5. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said software desired to be protected comprises a plurality of protected programs; each of said protected programs having validity information in a first predetermined location therein for indicating a valid identity of its rightful user exists in a second predetermined location therein , and an encrypted identity of its rightful user therein; and each of said protected programs, when being executed, will fail to operate if said validity information therein being altered, or said identity therein and the decryption result of said encrypted identity therein being inconsistent.

6. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 5, wherein said processing device having an encrypted identity of its rightful user ; and if one of said protected programs stored in said computer has a valid user identity which being not consistent with the decryption result of said encrypted identity of said processing device, use of said protected programs will not be permitted and will be permitted if otherwise .

7. (Third time Amended) Protection software for use on a processing device, to protect software publicly distributed by a system against unauthorised use ;

said protection software comprising :

identity software used on said processing device in enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of the user thereof for, when executed, providing user access to said software desired to be protected ;

wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually; and

wherein the improvement resides in said protection depends on no hardware specific to said user(s) and said identity software being specific to said rightful user(s) .

8. (First time Amended) Protection software as claimed in claim 7, wherein said operation being operation related to making payment from an account of said rightful user(s) .

9. (First time Amended) Protection software as claimed in claim 7, wherein said authorising software contains said identity software.

10. (Third time Amended) Authorising program/means used in a processing device, to protect other software against unauthorised use ;

said authorising program/means being for providing access to said software desired to be protected ;

wherein information specific to rightful user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said information being capable of being used, but not in a form to be so used , by said processing device in enabling operation(s) for which said rightful user(s) has to be responsible .

11. (First time Amended) Authorising program/means as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s).

12. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing device having an identity software/means ;

using said first information received being correct as a pre-condition for said processing device providing user access to said software desired to be protected;

wherein said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being ~~essentially~~ used by said processing device in enabling operation(s) for which said rightful user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

13. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said operation being operation related to making payment from an account of said rightful user(s) and said first information being a password.

14. (Second time Amended) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a control means of a processing device ;

using a favourable result of said authentication as a pre-condition for said control means providing user access to said software desired to be protected ;

wherein said identity information/means being used by said control means for enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) .

15. (First time Amended) A method for protecting software from unauthorised use , as claimed in claim 14, wherein said operation being operation related to making payment from an account of said rightful user(s).

16. (Third time Amended) A method for protecting software distributed by a system from unauthorised use , comprising the steps of :

a) creating first software with said confidential information of rightful user(s) of said software desired to be protected therein ;

b) running said first software on a processing device ;

c) obtaining by said first software running on said processing device , first information from the user thereof ;

d) determining by said first software, from said processing device second information related to the hardware or/and software thereof for future reference in step f) below, in response to said first information obtained being consistent with said confidential information therein ;

e) thereafter, authenticating by second software, the processing device onwhich said second software is being used, basing on at least a part of said second information ;

f) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

wherein said confidential information is necessary for enabling electronic transaction(s) for which said rightful user(s) has to be responsible ; and said steps c) to f) is being performed without causing a said transaction take place .

17. (First time Amended) A method for protecting software from unauthorised use, as claimed by claim 12, wherein said software desired to be protected being purchased commercial software.

18. (First time Amended) A method for protecting software from unauthorised use, comprising the steps of :

a) transferring from a software distribution system, said software desired to be protected to a processing device ;

b) transferring from said software distribution system, first and second software which being specific to a user, to said processing device ;

c) establishing a communication between said first software running on said processing device, and a control means of a remote electronic transaction system ;

d) verifying said user having a valid account, by said control means of said remote electronic transaction system to said first software ;

e) using by said first software, a favourable result of said verification as a pre-condition for determining from said processing device information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said user by said software distribution system, for the first time said steps a) to e) being carried out ; thereafter

f) authenticating by said second software, the processing device onwhich said second software is being used, say, second processing device, basing on at least a part of said information related to said hardware or/and software ;

g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing device, with no charge ;

if the result of said authentication is not favourable, repeat at least said steps c) to g) with said second processing device, without re-charging from said user said cost .

19. (First time Amended) A method for protecting softwarefrom unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to g) .

20. (Second time Amended) A method for protecting software distributed by a system from unauthorised use, comprising the steps of :

a) creating by said system, first software ;

wherein "the presence of identity information/means which being specific to a rightful user of said software desired to be protected and being used for enabling operation(s) for which said rightful user has to be responsible, in a processing device" ; is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

b) transferring from said system, said first software to said processing device ;

c) determining by said first software running on said processing device meeting said precondition, first information related to the hardware or/and software of said processing device , for future reference in step e) below ;

d) thereafter, determining by second software, from the processing device onwhich said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing device onwhich said second software is being used ;

repeat at least said steps c) to f) if said result of said determination of consistence is not favourable, without causing any operation(s) for which said rightful user has to be responsible, being performed ;

wherein said first and second software being specific to said rightful user.